Internal Security Act of 1950, which also brought subsections 793(d) and (e) into their present form.[403] As codified in 50 U.S.C. 783(b), it provides:

> It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

Subsection 783(b) is an important strand in the web of statutes governing revelation of defense secrets, although it has little bearing on proper construction of the espionage statutes. In the important *Scarbeck* case, the provision was construed to cover employee communications of classified material whether or not classification was proper in substance, so long as the manner of classification follows the procedural guidelines established by applicable Executive Orders.[404] It is clear from both the legislative history and this authoritative judicial construction that the sweep of the information subject to the statutory prohibition was thought justified by its narrow applicability with respect to actors and recipients.[405] No particular reading of the espionage statutes is implicit in the passage of 783(b), however, because 783(b) covers any classified information while the espionage statutes cover only material which a jury finds "related to the national defense." But it is notable that even with respect to a provision aimed solely at Government employees, Congress in 783(b) only prohibited communication to a very narrow category of recipients. The legislative history nowhere suggests that such communication would be deemed to have taken place through disclosure of classified information to the press, followed by widespread publication.

E. *The "Restricted Data" Statutes: 42 U.S.C. §§ 2271-81*

The interesting provisions which protect "restricted data"[406] concerning atomic weapons or energy from communication or disclosure to unauthorized

403. 64 Stat. 991 (1950).

404. Scarbeck v. United States, 317 F.2d 546, 558 (D.C. Cir.), *cert. denied*, 374 U.S. 856 (1963).

405. *Id.* at 559; Judge Washington's opinion for the D.C. Circuit contains an admirable treatment of the legislative history of 783(b), and we see no need to duplicate his efforts here.

406. "Restricted data" is defined in 42 U.S.C. 2014(y) as:

persons are of little assistance in construing the general espionage statutes, although they are of intrinsic significance in assessing controls on publication of defense information. Section 2274 sets out two differently graded offenses, the more severe being communication or disclosure of "restricted data" to anyone "with intent to secure an advantage to any foreign nation," and the second covering the same communication "with reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation."[407] The split of the culpability standards in these two subsections, and the different grading—in contrast to the culpability standards of the espionage statutes—indicate that recklessness, and perhaps negligence, with respect to injury or advantage is sufficient to violate these provisions. No purpose to injure or advantage presumably need be shown to establish a violation of the lesser offense. Section 2277 makes criminal knowing disclosure of restricted data to any person not authorized by the Atomic Energy Commission, but applies only to present and former Government employees or contractors.[408] Other sections make criminal receipt of restricted data with intent to injure the United States or to secure an advantage to any foreign nation,[409] and tampering with restricted data with like intent.[410]

One provision of possible relevance to the injunction proceeding against the New York Times is section 2280,[411] which authorizes injunctions against threatened violations of any of the criminal provisions governing restricted data. Presumably, section 2280 authorizes an injunction against a present or former Government employee planning on publishing himself, or revealing to a newspaper, restricted data. Such disclosure would violate section 2277. It is not clear, however, whether a newspaper could be enjoined from publication. Newspapers are not subject to section 2277, unless they are in conspiracy with the disclosing employee, and therefore are not subject to injunction by virtue of that substantive offense. Moreover, nothing in the legislative history bears on the question whether publication should be considered a communication "to any . . . person . . . with reason to believe such data will be utilized to injure the United States etc," in violation of subsection 2274(b). The arguments for and against such a construction generally follow our consideration of the meaning of communication in 793(d) and (e).[412]

These provisions and the legislative history which gave rise to them provide no insights into the meaning of the basic espionage statutes. We

all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 2162 of this title.

407. 42 U.S.C. § 2274 (1970).
408. 42 U.S.C. § 2277 (1970).
409. 42 U.S.C. § 2275 (1970).
410. 42 U.S.C. § 2276 (1970).
411. 42 U.S.C. § 2280 (1970).
412. *See* text following note 277 *supra*.

mention them briefly here to complete our overview of other statutes governing particular areas of information relating to the national security.

VIII. Conclusion: Room for Improvement

The basic espionage statutes are totally inadequate. Even in their treatment of outright spying they are poorly conceived and clumsily drafted. The gathering and obtaining offenses of subsections 793(a) and 793(b) have no underlying purpose that could not be served by more precise definition of attempts to violate the transmission offenses of subsection 794(a). No subsection of the general provisions of sections 793 or 794 has an easily understood culpability standard. Subsections 794(a), 793(a) and 793(b) employ "intent or reason to believe information is to be used to the injury of the United States or to the advantage of any foreign nation." Surely, however, Congress did not wish to subject negligent conduct to the death penalty by using the words "reason to believe"; nor is it clear what is meant by "is to be used" or "advantage" and "injury."

Subsection 793(c) is another puzzle. The culpability required turns on the meaning of the phrase "for the purpose aforesaid." The two sections immediately preceding it, subsections 793(a) and (b), state that conduct done "for the purpose of" obtaining information respecting the national defense, and with intent or reason to believe, is criminal. In light of the prior use of "purpose" and "intent" as separate requirements, the common-sense reading of subsection 793(c) is that "for the purpose aforesaid" means only "for the purpose of obtaining national defense information" and not "intent and reason to believe." Yet all the evidence we have found indicates agreement by both Congress and the Executive Branch that subsection 793(c) requires the same culpability as subsections 793(a) and (b).

Then, there are the mysteries of the term "willfully" in subsections 793 (d) and (e) and the added twist that a special "reason to believe" culpability requirement that allegedly protects in special fashion those who disclose "information," but not documents, is itself a problematic distinction. The phrase adds content to the law, however, only if the rest of the statute is read so broadly as to be clearly unconstitutional. Finally, there is 794(b)'s intent standard, which can be given a clear interpretation—intent means conscious purpose—only by making the statute paradoxical. Why did Congress choose to subject publications to controls pursuant to a standard that so rarely will be met? Why should actions taken by publications with the purpose of furthering foreign interests by disclosing national defense secrets not be criminal except in time of war? In light of this confusion about the culpability standards, it is somewhat ironic to recall the confident assertions in *Gorin* that the vague

parameters of "national
is required.

The difficulty in fi
espionage is minor comp
of criminal responsibilit
fense secrets. In essence
broad statutory languag
erable evidence spread
limited prohibitions. Th
congressional intent is
stood by lawmakers who
one another over the me
criminality of public del
neither the Congresses t
them have behaved in a
pionage statutes forbid a
the absence of additional

Regardless of the p
for clarification by legisl
the current law is tolera
and publish have been so
the deeper significance of
the passing of an era in w
reasonably well understoo
deemed sensitive. As rema
the Executive Branch sin
the general discretion wit
to the naturally symbiotic
New York Times, by pub
bate within the Executive
no longer willing to be
common aims, but intend
not only political dogma b
Times should be discreet,
lish anything that the Time

413. *See* The New Yor
History 397 (Comp. by J. Goo
414. The most famous re
the upcoming Bay of Pigs v
(1972). More significant perh
official censorship of the press.
415. Thus, Ramparts pri
success in breaking the codes
U.S. Electronic Espionage: A

parameters of "national defense information" may be ignored because scienter is required.

The difficulty in finding the proper application of the laws to clandestine espionage is minor compared to the incredible confusion surrounding the issue of criminal responsibility for collection, retention, and public disclosure of defense secrets. In essence, a choice must be made between giving effect either to broad statutory language designed in the Executive Branch or to the considerable evidence spread over a half-century that Congress wanted much more limited prohibitions. The choice is particularly difficult since the evidence of congressional intent is not absolutely clear. Issues were not precisely understood by lawmakers who were often unenlightened and at cross-purposes with one another over the meaning of basic terms. Nevertheless, on the issue of the criminality of public debate, one proposition is, in our view, unquestionable: neither the Congresses that wrote the laws nor the Executives who enforced them have behaved in a manner consistent with the belief that the general espionage statutes forbid acts of publication or conduct leading up to them, in the absence of additional and rarely present bad motives.

Regardless of the proper construction of the current statutes, it is time for clarification by legislation that treats the problem anew. The ambiguity of the current law is tolerable only because the limits of the right to disclose and publish have been so rarely tested. This pressing to the limits is, in a sense, the deeper significance of the publication of the Pentagon Papers. It symbolizes the passing of an era in which newsmen could be counted upon to work within reasonably well understood boundaries in disclosing information that politicians deemed sensitive. As remarkable as the constant flow of leaked information from the Executive Branch since the classification programs were implemented[413] is the general discretion with which secret information has been used[414] (attesting to the naturally symbiotic relationship between politicians and the press). The New York Times, by publishing the Papers, did not merely reveal a policy debate within the Executive Branch; it demonstrated that much of the press was no longer willing to be merely an occasionally critical associate devoted to common aims, but intended to become an adversary threatening to discredit not only political dogma but also the motives of the nation's leaders. And if the Times should be discreet, some underground newspaper stands ready to publish anything that the Times deems too sensitive to reveal.[415]

413. *See* THE NEW YORK TIMES COMPANY V. UNITED STATES: A DOCUMENTARY HISTORY 397 (Comp. by J. Goodale, 1971) (affidavit of Max Frankel) (1971).

414. The most famous recent case is the New York Times' decision not to report the upcoming Bay of Pigs venture. S. UNGAR, THE PAPERS AND THE PAPERS 101-02 (1972). More significant perhaps, the United States fought World War II without any official censorship of the press.

415. Thus, Ramparts printed claims that the United States has had remarkable success in breaking the codes of the U.S.S.R., a matter of great importance if true. *See U.S. Electronic Espionage: A Memoir*, RAMPARTS, August, 1972, at 35.

Village Voice

This changing role of the press is a necessary counterweight to the increasing concentration of the power of government in the hands of the Executive Branch. There are, however, aspects to the development that are troublesome in the context of national defense secrets. We reject the utopian notion that there are no defense secrets worth keeping and that every aspect of national security should be disclosed to facilitate adequate public comprehension of the policy choices to be made. Yet technology makes document copying ever more simple. As the lower levels of the executive bureaucracy, shut off from real participation in decision-making, are racked by the same conflicts about the ends and means of foreign policy that characterize the wider community, criminal sanctions assume greater significance in the protection of the Government's legitimate secrecy interests. Paradoxically, the likely consequence of the law's failure to give weight to security considerations would be to augment the strong tendency to centralize power into fewer hands, because only a small group can be trusted to be discreet.

If regulation of publication is necessary, it is far better for Congress to do the job than to permit the Executive Branch to enforce secrecy by seeking injunctive relief premised upon employee breach of adhesion contracts. In the recent *Marchetti* case,[416] a former C.I.A. agent was enjoined from publishing, without prior agency approval, accounts of his experience as an intelligence agent.[417] He had signed an agreement as a condition of employment saying that he would never reveal "information related to the national defense."[418] Although the policy of requiring government officials, past and present, to remain silent may be wise, it is not a question that ought to be relegated to judicial enforcement of executive contracts, thereby excluding from policy formation the one branch most entitled to decide. Only the fact that the

416. United States v. Marchetti, 466 F.2d 1309 (4th Cir.), *cert. denied*, 93 S. Ct. 553 (1972).

417. The Court held that the C.I.A. might disapprove publication only of matters that were both classified and had not been publicly disclosed. But "rumor and speculation are not the equivalent of prior disclosure. . . ." 466 F.2d at 1318. Opportunity for judicial review of the propriety of classification was denied. *Id.*

418. 466 F.2d at 1312. The agreement stated, in part:

> 1. I, Victor L. Marchetti, understand that by virtue of my duties in the Central Intelligence Agency, I may be or have been the recipient of information and intelligence which concerns the present and future security of the United States. This information and intelligence, together with the methods of collecting and handling it, are classified according to security standards set by the United States Government. I have read and understand the provisions of the espionage laws, Act of June 25, 1948, as amended, concerning the disclosure of information relating to the National Defense and I am familiar with the penalties provided for violation thereof.
>
> 2. I acknowledge, that I do not now, nor shall I ever possess any right, interest, title or claim, in or to any of the information or intelligence or any method of collecting or handling it, which has come or shall come to my attention by virtue of my connection with the Central Intelligence Agency, but shall always recognize the property right of the United States of America, in and to such matters.

The agreement does not reflect current law on either our, or apparently the C.I.A.'s, reading of it. *See* Memorandum of the Central Intelligence Agency entitled "The Espionage Laws" by M. G. Miskovsky, Assistant General Counsel, 1961. (Copy on file at Columbia Law Library).

Government will so ra
Marchetti precedent fo
tive to the necessity of l

The opportunity f
hand, since Congress i
of the federal criminal
present federal crimina
that inevitably occur w
ceptual clarity and ove
Congresses.[419] But rev
to matters like espiona
plored in the course of
nately, the espionage p
and S. 1400,[421] the Ni
reconcile the conflicting
ferent espionage propo
to come, general discu
proposals seems more a

The basic problem
old law is perpetuated
that perplexed former
sections 793-98 with the

§ 2-5B7. Espiona

(a) OFFENSE
(1) with
the injury of
power, he gat
tion for or to a
(2) with
in time of wa
wise communi
(b) ATTEMPT
section 1-2A4 (cri
to constitute a sub
sion of espionage

419. *Cf.* Wechsler, *Th*
(1952).

420. S. 1, 93d Cong.,
lengthiest ever introduced,
THE NATIONAL COMMISSIO
FEDERAL CRIMINAL CODE (1

421. S. 1400, 93d Cong.

422. In addition to the
Print leading to S. 1, the
OF FEDERAL CRIMINAL LA
(1971) and the COMMISSIO
(1970).

Government will so rarely have advance notice of intent to publish keeps the *Marchetti* precedent for injunctive relief from becoming a dangerous alternative to the necessity of legislative clarification.

The opportunity for careful reevaluation of the espionage problem is at hand, since Congress is now considering the recodification and reformulation of the federal criminal law. Few undertakings deserve greater support. The present federal criminal law suffers generally from the confusion and defects that inevitably occur when major problems in the law of crimes requiring conceptual clarity and overall design are left to the ad hoc responses of successive Congresses.[419] But revision is a task of awesome complexity, particularly as to matters like espionage where the underlying problems have not been explored in the course of recent efforts to revise state criminal codes. Unfortunately, the espionage proposals currently before Congress as part of S. 1[420] and S. 1400,[421] the Nixon Administration's latest proposal, are inadequate to reconcile the conflicting interests at stake. Insofar as there have been five different espionage proposals[422] in the last two years, and there are surely more to come, general discussion of the approach of the two most recent revision proposals seems more appropriate than detailed analysis.

The basic problem with S. 1 is that too much of the sloppy drafting of the old law is perpetuated and the new formulations do not resolve the problems that perplexed former Congresses. S. 1 treats the matters now covered by sections 793-98 with the following provisions:

> § 2-5B7. Espionage
>
> (a) OFFENSE.—A person is guilty of espionage if:
>
> (1) with knowledge that the information is to be used to the injury of the United States or to the advantage of a foreign power, he gathers, obtains, or reveals national defense information for or to a foreign power or an agent of such power; or
>
> (2) with intent that it be communicated to the enemy and in time of war, he elicits, collects, records, publishes, or otherwise communicates national defense information.
>
> (b) ATTEMPT.—Without otherwise limiting the applicability of section 1-2A4 (criminal attempt), any of the following is sufficient to constitute a substantial step under such section toward commission of espionage under subsection (a)(1): obtaining, collecting, or

419. *Cf.* Wechsler, *The Challenge of a Model Penal Code*, 65 HARV. L. REV. 1097 (1952).

420. S. 1, 93d Cong., 1st Sess. §§ 2-5A1, 2-5B7-8 (1973). The bill, reputedly the lengthiest ever introduced, is derived, with substantial changes, from the FINAL REPORT OF THE NATIONAL COMMISSION ON REFORM OF FEDERAL CRIMINAL LAWS, PROPOSED NEW FEDERAL CRIMINAL CODE (1971).

421. S. 1400, 93d Cong., 1st Sess. §§ 1121-26 (1973).

422. In addition to the current S. 1 and S. 1400, see §§ 2-5B7-8 in the Committee Print leading to S. 1, the FINAL REPORT OF THE NATIONAL COMMISSION ON REFORM OF FEDERAL CRIMINAL LAWS, PROPOSED NEW FEDERAL CRIMINAL CODE, §§ 1112-1116 (1971) and the COMMISSION'S STUDY DRAFT OF A NEW FEDERAL CRIMINAL CODE §§ 1113-6 (1970).

eliciting national defense information, or entering a restricted area to obtain such information.

(c) GRADING.—The offense is a Class A felony if committed in time of war or if the information directly concerns military missiles, space vessels, satellites, nuclear weaponry, early warning systems or other means of defense or retaliation against attack by a foreign power, war plans, or defense strategy. Otherwise it is a Class B felony.

§ 2-5B8. Misuse of National Defense Information

(a) OFFENSE.—A person is guilty of an offense if in a manner harmful to the safety of the United States he:

(1) knowingly reveals national defense information to a person who is not authorized to receive it;

(2) is a public servant and with criminal negligence violates a known duty as to custody, care, or disposition of national defense information, or as to reporting an unauthorized removal, delivery, loss, destruction, or compromise of such information;

(3) knowingly having unauthorized possession of a document or thing containing national defense information, fails to deliver it on demand to a Federal public servant entitled to receive it;

(4) knowingly communicates, uses, or otherwise makes available to an unauthorized person communications information;

(5) knowingly uses communications information; or

(6) knowingly communicates national defense information to an agent or representative of a foreign power or to an officer or member of an organization which is, in fact, defined in section 782(5), title 50, United States Code.

(b) GRADING.—The offense is a Class C felony if it is committed in time of war. Otherwise it is a Class D felony.

The key term "national defense information" is explicitly defined:

"[N]ational defense information" means information regarding:

(i) the military capability of the United States or of a nation at war with a nation with which the United States is at war;

(ii) military or defense planning or operations of the United States;

(iii) military communications, research, or development of the United States;

(iv) restricted data as defined in section 2014, title 42, United States Code;

(v) communications information;

(vi) in time of war, any other information which if revealed could be harmful to national defense and which might be useful to the enemy;

(vii) defense intelligence of the United States, including information relating to intelligence operations, activities, plans, estimates, analyses, sources, and methods.

In our opinion, enactment of this proposal would do no more than perpetuate the current confused state of the law. Consider the espionage

offenses of section 2-5B7, which for the most part restates the current section 794. Like subsections 794(a) and (b), the two offenses created are nearly identical. Section (a)(1) makes knowledge that national defense information "is to be used" to the injury of the United States or to the advantage of a foreign nation the test of whether a crime is committed. Does one who publishes "reveal . . . for or to a foreign power" within the meaning of the law? If not, it is only because 2-5B7(a)(2) says "publishes" while (a)(1) does not. Whatever the proper resolution, it is a mistake for recodification to treat such an important issue so opaquely. Similarly, publishing is explicitly made criminal only in time of war and only where there is "intent that [the information] be communicated to the enemy." The proposed code defines "intentionally" to require a conscious objective to cause the particular result.[423] Consequently, as in 794(b), the purported coverage of publication is largely illusory because very few newspapers intend to inform the enemy.

The new offense of "Misuse of National Defense Information" in section 2-5B8 is also perplexing, although we can be thankful that it departs from the models set out by section 793, particularly in its dispatching with the entitlement concept. Is publishing or conduct incident thereto meant to be covered? What is the meaning of "in a manner harmful to the safety of the United States?" Aside from issues of vagueness, is this phrase intended to require that the prosecutor prove that because of the actor's conduct consequences harmful to United States' safety actually resulted, were likely to result or might conceivably have come about?[424] To ignore clear resolution of these issues is to be satisfied with a statute whose basic design defies interpretation.

The Administration's proposals in S. 1400 do not suffer from these ambiguities. Their problem is that they are so excessively restrictive of public debate that their unconstitutionality, let alone their misconceptions of appropriate public policy, is, in our view, patent. Five offenses, too lengthy to be fully set out, are defined: espionage,[425] disclosing national defense information,[426] mishandling national defense information,[427] disclosing classified information,[428] and unlawfully obtaining classified information.[429] The proposed espionage offense is drafted with remarkable breadth:

> (a) OFFENSE.—A person is guilty of an offense, if, with intent that information relating to the national defense be used, or with knowledge that it may be used, to the prejudice of the safety or interest

423. S. 1, 93d Cong., 1st Sess. § 1-2A1(a)(2) (1973).

424. Whether the statute is intended to achieve the results it does is problematic. Note for example, that it would repeal section 793(e)'s retention offense. In addition, the treatment of communications information, earlier defined as "national defense information" is either redundant or hopelessly opaque.

425. S. 1400, 93d Cong., 1st Sess. § 1121 (1971).

426. *Id.* at § 1122.

427. *Id.* at § 1123.

428. *Id.* at § 1124.

429. *Id.* at § 1125.

of the United States, or to the advantage of a foreign power, he knowingly:

> (1) communicates such information to a foreign power;
> (2) obtains or collects such information for a foreign power or with knowledge that it may be communicated to a foreign power; or
> (3) enters a restricted area with intent to obtain or collect such information for a foreign power or with knowledge that it may be communicated to a foreign power.

Insofar as "communicate" means "to make information available by any means, to a person or to the general public,"[430] the statute makes it an offense to collect national defense information knowing that it may be published.[431] "National defense information" is defined slightly more narrowly than in S. 1, but does include:

> [I]nformation, regardless of its origin, relating to:
>
> (1) the military capability of the United States. . . .
> * * * *
> (5) military weaponry, weapons development, or weapons research of the United States. . . .
> * * * *
> (9) the conduct of foreign relations affecting the national defense. . . .[432]

Given the scope of "national defense information," the result would be to paralyze newspaper reporting on national defense affairs. We strongly doubt that the nation needs a far reaching official military secrets act. Surely it does not need one that makes the offense a capital crime when committed "during a national defense emergency" or when information concerns a "major weapons system or [a] major element of defense strategy,"[433] and a class B felony otherwise.[434]

Similarly, the rest of the offenses, with the exception of obtaining classified information,[435] are defined in terms so broad that they mark an abrupt departure from statutory precedents. Any knowing communication of defense information to an unauthorized person would be made a class C or D felony,

430. *Id.* at § 1126(c).

431. It is difficult for us to believe that this was intended. It nonetheless is the technical result of the statute in that he who "obtains or collects" information "with knowledge" that it "may" be used to the advantage of a foreign power, and knowing that it "may be communicated to a foreign power" commits the highest offense.

432. S. 1400, 93d Cong., 1st Sess. § 1121, § 1126(g) (1971).

433. *See* § 2401(a)(1)(B). The death penalty is mandatory if the defendant "knowingly created a grave risk of substantial danger to the national security" and mitigating factors not likely to be present in publication are absent.

434. *Id.* at § 1121(b). Class B felonies are punishable by a maximum of 30 years imprisonment. § 2301(b)(2).

435. *Id.* at § 1125. It applies only to agents of foreign powers. Classified information is defined, § 1126(b), as "information, regardless of its origin," which is marked by statute, or pursuant to executive order or implementing rules or regulations as "information requiring a specific degree of protection against unauthorized disclosure for reasons of national security."

and unauthorized retainir
both without regard to a
United States.[436] Disclos
federal employee, except t
pursuant to "lawful dema
that information was impr

The consequence of
all public and private spee
tors and juries to choose
criticism of our defense a
we can only marvel that le
be seriously proposed. We

What should be done
newspapers reveal large an
and exceedingly expensive
own. That form of foreign
quence of the nation's deep
protests that as a general
strength[440] because our str
concern the protection of s
tives, opportunities, and ac
publicized.[441] Unfortunatel
whether they can effectivel
we have about intelligence
security interests have been
nonetheless come to certain
lators and others in their c

No legislation can be
problems must be treated
ex-employees, and newspape

436. *Id.* at §§ 1122(b), 1123
years imprisonment § 2301(b)(
years imprisonment, § 2301(b)(

437. *Id.* at § 1124(a)(c)(e
years imprisonment § 2301(b)(
is left unexplained.

438. *Id.* at § 1124(d).

439. *Cf.* United States v. R
'national defense' is the notion
Nation apart."

440. *See, e.g.*, A. DULLES, T

441. The archtypical case is
ently, developments in codes mak
equipment may be used. For a
THE CODEBREAKERS (1967).

442. Additionally, it may be
public revelations from private one

and unauthorized retaining of defense information would be a class D felony, both without regard to any intention or knowledge respecting injury to the United States.[436] Disclosure of classified information by a present or former federal employee, except to a "regularly constituted" Congressional committee pursuant to "lawful demand," would be a Class E felony[437] and no defense that information was improperly classified would be permitted.[438]

The consequence of S. 1400's enactment would be to prohibit virtually all public and private speech about national defense secrets, leaving to prosecutors and juries to choose victims among those who engage in reporting and criticism of our defense and foreign policies. Like Senator Cummins in 1917, we can only marvel that legislation at once so sweeping and so stringent could be seriously proposed. We trust that it will not be enacted.

What should be done? In our reasonably open society, Congress and the newspapers reveal large amounts of defense information that would be difficult and exceedingly expensive for interested foreign governments to collect on their own. That form of foreign aid to adversaries is, however, a necessary consequence of the nation's deepest values.[439] We do not accord much significance to protests that as a general matter we make it easy for others to assess our strength[440] because our strength is so awesome. The more difficult questions concern the protection of secrecy in narrower premises where specific objectives, opportunities, and advantages are lost if particular types of secrets are publicized.[441] Unfortunately, to distinguish these matters—indeed to know whether they can effectively be distinguished—requires more knowledge than we have about intelligence affairs and the extent to which truly important security interests have been compromised by well-meant disclosures. We have nonetheless come to certain conclusions that, while general, may assist legislators and others in their consideration of the problems.

No legislation can be adequate unless it recognizes that at least three problems must be treated independently: spies, government employees and ex-employees, and newspapers and the rest of us.[442] Both the present espionage

436. *Id.* at §§ 1122(b), 1123(b). Class C felonies are punishable by a maximum of 15 years imprisonment § 2301(b)(3); class D felonies are punishable by a maximum of 7 years imprisonment, § 2301(b)(4).

437. *Id.* at § 1124(a)(c)(e). Class E felonies are punishable by a maximum of 3 years imprisonment § 2301(b)(5). How Congress can "demand" what it is ignorant of is left unexplained.

438. *Id.* at § 1124(d).

439. *Cf.* United States v. Robel, 389 U.S. 258, 264 (1967): "Implicit in the term 'national defense' is the notion of defending those values and ideals which set this Nation apart."

440. *See, e.g.*, A. DULLES, THE CRAFT OF INTELLIGENCE 241-247 (1963).

441. The archtypical case is revelation that a foreign code has been broken. Apparently, developments in codes make that prospect increasingly unlikely where sophisticated equipment may be used. For a fascinating discussion of code-breaking, see D. KAHN, THE CODEBREAKERS (1967).

442. Additionally, it may be wise to differentiate employees from ex-employees, and public revelations from private ones.

statutes and the proposals of S. 1 and S. 1400[443] are fatally defective in that they ignore the necessity of separate considerations of the distinct interests in each of these contexts.

The essence of classical espionage is the individual's readiness to put his access to information of defense significance at the disposal of agents of foreign political organizations. Granted that the harm that results from his conduct is a function of the importance of the information transferred, there should be no hesitation, regardless of the banal quality of defense information involved, to punish the citizen whose priorities are so ordered or foreigners whose job it is to risk apprehension. We believe, therefore, that the information protected against clandestine transfer to foreign agents should be defined broadly, probably more broadly than in current law. In this context, we see no dispositive objection to making knowing and unauthorized transfer of classified information to foreign agents an offense, without regard to whether information is properly classified.[444] That a spy might earn complete immunity by stealing secrets so serious that their significance cannot be disclosed in court—a clear possibility under current law,[445] and also under S. 1 and S. 1400—is an outcome that should be avoided, if possible.

Two objections may be made to this broadened approach. First, it puts considerable reliance on the capacity to adjudicate accurately whether persons are in fact acting as agents of foreigners. If the prosecutor need not demonstrate the significance of the transferred information, there is an enhanced risk that casual disclosures of improperly classified information to foreign friends may be wrongly deemed espionage. Nothing in the literature, however, suggests to us that this is a serious problem, and it may be further minimized by insistence upon the actor's awareness that his disclosures are intended for primary use by foreign political organizations.[446] Second, and more troublesome to us, is the fact that for deterrence purposes the penalties for espionage are and should be exceptionally steep. Denying improper classification as a defense may expose an offender whose conduct has produced no real harm to the most serious penalties the law permits. To avoid this result the law might expressly authorize *in camera* sentencing proceedings, or, preferably to us, make the offense substantially less serious if the Government is unprepared to disclose the underlying significance of the material transferred.

Quite different issues are posed by revelations of defense secrets by government employees or ex-employees. Prohibiting employees from telling

443. In structure, S. 1400 is preferable to S. 1 in that it does differentiate government employment as a problem to be treated separately from espionage proper. Its failure is that it treats newspapers with a severity appropriate for spies.

444. We thus disagree with the analysis in I WORKING PAPERS OF THE NATIONAL COMMISSION ON REFORM OF FEDERAL CRIMINAL LAWS, 454-55 (1970).

445. *See* text following note 124 *supra*.

446. If necessary, special protection for government servants authorized to negotiate with foreign governments might be created.

1973]

what they know at pain
of information to the publi
less, to say that any gover
reveal anything he choos
accords too little weight to

In our opinion some
are no doubt exceptionall
principles provide approp
ployee disclosures to Con
S. 1400.[447] Second, no ma
legislation should explici
jury either to balance the
tance for public understa
of duty by the employee's
that the employee serves

Third, the informatio
be narrower than that pr
disagree with S. 1400's d
than espionage provisions
penalties are less severe t
is the reverse: espionage
severity is better cured b
striction of the informatic
ernment proof of defense
what the Government is
is to find standards to de
the public. Certainly the f
substantial overclassificat
official secrecy.[450] Impro

447. There are obviously
insofar as revelation to a pa
to public revelation immuni
independent congressional inv

448. Any such defenses
further. Nonetheless, there a
rant the disclosure of defens
characterizing the problem a

449. To be sure, the em
contemplating espionage.

450. For recent reports
Information Policies and Pr
House Comm. on Governmen
head Hearings).

There are numerous pos
ticularly automatic declassifi
For proposals, see McHUG
CLASSIFYING GOVERNMENT I
multiple reasons, some good
think substantial overclassifi

what they know at pain of criminal punishment obviously restricts the flow of information to the public and impairs the quality of public debate. Nonetheless, to say that any government employee or former employee is privileged to reveal anything he chooses at risk of sanctions no greater than dismissal accords too little weight to the need for security.

In our opinion some middle ground should be sought. Although statutes are no doubt exceptionally difficult to formulate, we think that the following principles provide appropriate guides to future legislative efforts. First, employee disclosures to Congress should be protected more rigorously than in S. 1400.[447] Second, no matter what information is protected against revelation, legislation should explicitly provide a justification defense, permitting the jury either to balance the information's defense significance against its importance for public understanding and debate, or to consider possible dereliction of duty by the employee's superiors.[448] To do otherwise would not recognize that the employee serves both the Government and the public.

Third, the information that is protected against employee revelation should be narrower than that protected against espionage. On this point we strongly disagree with S. 1400's drafting of simple disclosure proposals more broadly than espionage provisions, apparently on the misguided notion that since the penalties are less severe the conduct covered may be broader.[449] Our approach is the reverse: espionage has no claim to the law's sympathy and excessive severity is better cured by flexible grading of the offense than by narrow restriction of the information protected against transfer, which necessitate Government proof of defense significance. By contrast, informing the public of what the Government is doing is presumptively desirable. The hard problem is to find standards to define what limited information cannot be revealed to the public. Certainly the fact of classification should not be determinative since substantial overclassification is inevitable given the variety of inducements to official secrecy.[450] Improper classification must be a defense, and, if possible,

447. There are obviously exceedingly difficult issues to be resolved here, particularly insofar as revelation to a particular Senator or Congressman may be merely a conduit to public revelation immunized by congressional privilege, rather than a prelude to independent congressional investigation.

448. Any such defenses may result in lengthening trials and compromising security further. Nonetheless, there are clearly instances where broader duties to the public warrant the disclosure of defense information and where the issue would be confused by characterizing the problem as one of improper classification.

449. To be sure, the employee has obligations of loyalty, but so does the citizen contemplating espionage.

450. For recent reports on overclassification, see *Hearings on U.S. Government Information Policies and Practices—The Pentagon Papers—Before a Subcomm. of the House Comm. on Government Operations*, 92d Cong., 1st Sess. pts. 1-3, 7 (1971) (Moorhead Hearings).

There are numerous possible treatments of the problem of overclassification, particularly automatic declassification of nearly everything after an arbitrary time period. For proposals, see McHUGH, PROPOSED ALTERNATIVES TO THE PRESENT SYSTEM OF CLASSIFYING GOVERNMENT DOCUMENTS. *Id.* at 2293. Nonetheless, given that there are multiple reasons, some good and some bad, why Government officials want secrecy, we think substantial overclassification is inevitable.

protected information should be defined even more narrowly and without direct reference to classification. Thus, even if the Constitution permits penalizing employee or ex-employee disclosure of any information that the Government is not legally obligated to reveal,[451] we think such a secretive position should be rejected as a matter of policy. Fourth, the offense of revealing protected information should be graded to respect the differences between loose talk and intentional efforts to compromise security.

Finally, there are the problems of the press and those who disclose defense information in the course of public and private discussion. The claim may be made that lines should be drawn in the same place as for government employees.[452] It may seem paradoxical to provide the press with the privilege of publishing the fruits of a crime, a result that inevitably occurs if more information is protected against employee disclosure than against publication. Nevertheless, it seems to us that an asymmetry of obligations between public servants and the rest of us should be preserved, at least until such time as far-reaching institutional changes are made in congressional access to defense information. Congress has no assured access to security information and no sense of entitlement to it, as the inability of the Foreign Relations Committee to secure the Pentagon Papers demonstrates.[453]

Consequently, one cannot at the present time have confidence that more than a single elected official, if that, has given consent to whatever policy may be compromised by newspaper disclosure of defense information. Given that situation, doubts whether to protect the political efficacy of disclosure rather than stress its adverse security consequences should be resolved on the side of public debate. Peacetime prohibition of newspaper disclosure and citizen communication should be left to the most narrowly drawn categories of defense information such as the technical design of secret weapons systems or information about cryptographic techniques. Even as to such narrow categories of defense-related information, however, it is as true today as it was in 1917 that any item of information could, in some circumstances, have significance for public debate which outweighs any adverse effect on national security. Thus, prohibitions against newspaper and citizen disclosure applicable only to very

451. *Cf.* Environmental Protection Agency v. Mink, 93 S. Ct. 827 (1973).

452. *Cf.* Henkin, *The Right to Know and the Duty to Withhold: The Case of the Pentagon Papers* 120 U. PA. L. REV. 271, 278-79 (1971).

453. *See* S. UNGAR, *supra* note 3 at 69-71. Two intriguing aspects of the *New York Times* litigation were first, the Government's prompt concession in court that much of the material could be immediately declassified, and second, the claim that considerable time should be granted to winnow out the truly important information among that which was potentially sensitive. Both propositions provide insight on the seriousness with which Senator Fulbright's repeated requests were treated.

This is a central difference between the secrecy situation in Great Britain and our own. The British Official Secrets Act provides far greater protection for Government secrecy than do our espionage laws. But in Great Britain, the persons with principal executive authority and access to secrets sit as elected officials, and their comments in Parliament are privileged, providing greater assurance against policies gone wild.

narrow categories of information should also provide for a justification defense turning on superceding importance for public debate.

The dangers endemic to the administration of such a justification defense should not be minimized. Juries may be inclined to accord weight to the respectability and influence of a media defendant in assessing the justification for publication of the particular defense information. Selective enforcement is a real danger. Moreover, predictability will largely be sacrificed with a resulting chill on publication that should be justifiable in the legal sense. But uncertainty in the application of legal standards to publication of defense information is the price of rejecting simplistic solutions to the problem. Neither prohibiting nor privileging the publication of categories of defense information across the board does justice to the vital and competing social interests in secrecy and public revelation.

We have lived throughout the present century with extraordinary confusion about the legal standards governing publication of defense information. Clarification of the standards is now called for. However, uncertainties in the administration of theoretically sound legislative solutions should not force us to choose between extreme and simplistic policies. If the choice is narrowed to extremes, we hope that our current lawmakers exhibit the fortitude of their predecessors in 1917 who resisted the sweeping proposals of the Wilson Administration.